This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently amended) An authentication system for authenticating a user's signature as electronically inputted into a system by a manual input device providing an output indicative of its location with respect to time when manipulated by the user, the system comprising:

a first extraction means for extracting angle and distance data relating to different parts of the user's signature inputted into the system by the manual input device to obtain a signature trace;

normalization means for normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and a total time to produce the signature to 1;

a second extraction means for extracting angle and distance data relating to different parts of the normalized signature trace;

registration means for setting up a reference data file comprising angle and distance data extracted from a plurality of samples of the user's signature inputted into the system by the user by means of the manual input device during a registration phase;

comparison means for comparing the angle and distance data extracted by the second extraction means from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria; and

verification means for providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison.

2. (Previously presented) A system according to claim 1, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature as inputted into the system by the manual input device.

3. (Previously presented) A system according to claim 2, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating each of a number of said points to an immediately preceding point in the user's signature as inputted into the system by the manual input device.

4. (Previously presented) A system according to claim 2 or 3, wherein the second extraction means is adapted to extract data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature as inputted into the system by the manual input device.

5. (Previously presented) A system according to claim 1, wherein the second extraction means includes angle extract means for extracting angle data concerning the relative angular positions of a plurality of points of the user's signature.

6. (Previously presented) A system according to claim 1, wherein the second extraction means includes distance extract means for extracting distance data concerning the relative distances apart of a plurality of points of the user's signature.

7. (Previously presented) A system according to claim 1, wherein the second extraction means includes timing extract means for extracting timing data indicative of the relative times between execution of different parts of the user's signature, and the comparison means is adapted to compare the extracted timing data with reference timing data in the reference data file.

8. (Previously presented) A system according to claim 1, wherein password verification means is provided for verifying input of a required password, as determined by reference password means, by the user using a keyboard input device.

9. (Original) A system according to claim 8, wherein timing verification means is provided for verifying input of the password by the user with the required timing, as determined by reference timing means, using the keyboard input device.

10. (Previously presented) A system according to claim 9, wherein the timing verification means includes means for verifying a plurality of hold times for which the relevant keys of the keyboard input device are depressed during input of the password, and means for verifying a plurality of latency times between a release of one key and a depression of a following key during use of the keyboard input device to enter the password.

11. (Previously presented) A system according to claim 1, wherein user name input means is provided for receiving a user name inputted into the system to identify the identity of the user for the purposes of selection of the required reference data file for that user.

12. (Currently amended) A system according to claim 1, wherein the comparison means incorporates at least one neural network for determining the verification criteria by which a match is to be judged by providing a comparison output to the verification means.

13. (Previously presented) A system according to claim 1, wherein the second extraction means is adapted to extract data relating to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

14. (Original) A system according to claim 13, wherein the fitness function is optimised by an optimisation algorithm, such as a genetic algorithm.

15. (Previously presented) A system according to claim 1, further comprising a training means for training the system to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature inputted into the system by the user during the registration phase and generated false samples.

16. (Previously presented) A system according to claim 1, wherein the verification means is adapted to provide a reject output indicative of non-matching of one or more verification criteria only after completion of all the verification procedures.

17. (Currently amended) A method for authenticating a user's signature as electronically inputted into a system by a manual input device providing an output indicative of its location with respect to time when manipulated by the user, comprising:

extracting angle and distance data relating to different parts of the user's signature inputted into the system by the manual input device to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and the total time to produce the signature to 1;

extracting angle and distance data relating to different parts of the normalized signature trace;

creating a reference data file comprising angle and distance data extracted from a plurality of samples of the user's signature inputted into the system by the user using a manual input device during a registration phase;

comparing the angle and distance data extracted from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria; and

providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison.

18. (Previously presented) The method of claim 17, wherein extracting angle and distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating some of said points to other points in the user's signature as inputted into the system by the manual input device.

19. (Previously presented) The method of claim 18, wherein extracting angle and distance data comprises extracting data relating to a plurality of different points of the user's

signature including data relating each of a number of said points to an immediately preceding point in the user's signature as inputted into the system by the manual input device.

20. (Previously presented) The method according to claim 18 or 19, wherein extracting angle and distance data comprises extracting data relating to a plurality of different points of the user's signature including data relating a last point to a first point in the user's signature as inputted into the system by the manual input device.

21. (Previously presented) The method of claim 17, wherein extracting angle and distance data includes extracting angle data concerning the relative angular positions of a plurality of points of the user's signature.

22. (Previously presented) The method of claim 17, wherein extracting angle and distance data includes extracting distance data concerning the relative distances apart of a plurality of points of the user's signature.

23. (Previously presented) The method of claim 17, wherein extracting angle and distance data includes extracting timing data indicative of the relative times between execution of different parts of the user's signature, and the comparison means is adapted to compare the extracted timing data with reference timing data in the reference data file.

24. (Previously presented) The method of claim 17, further comprising verifying an input of a required password, as determined by reference password, by the user using a keyboard input device.

25. (Previously presented) The method of claim 24, further comprising verifying the input of the password by the user with a required timing, as determined by a reference timing, using the keyboard input device.

26. (Previously presented) The method of claim 25, wherein verifying the input further comprises:

verifying a plurality of hold times for which the relevant keys of the keyboard input device are depressed during input of the password; and

verifying a plurality of latency times between the release of one key and the depression of the following key during use of the keyboard input device to enter the password.

27. (Previously presented) The method of claim 17, further comprising receiving a user name inputted into the system to identify the identity of the user for the purposes of selection of the required reference data file for that user.

28. (Currently amended) The method of claim 17, wherein comparing the angle and distance data incorporates at least one neural network for determining the verification criteria by which a match is to be judged by providing a comparison output to the verification means.

29. (Previously presented) The method of claim 17, wherein extracting angle and distance data extracts data relating to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

30. (Previously presented) The method of claim 29, wherein the fitness function is optimised by an optimisation algorithm, such as a genetic algorithm.

31. (Previously presented) The method of claim 17, further comprising training to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature inputted by the user during the registration phase and generated false samples.

32. (Previously presented) The method of claim 17, wherein providing verification of the user's signature provides a reject output indicative of non-matching of one or more verification criteria only after completion of all the verification procedures.

33. (Currently amended) A method for authenticating a user's signature as electronically inputted into a system by a manual input device providing an output indicative of its location with respect to time when manipulated by the user, comprising:

extracting angle and distance data relating to different parts of a user's signature inputted device to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and the total time to produce the signature to 1; and

extracting angle and distance data relating to different parts of the normalized signature trace.

34. (Previously presented) The method of claim 33, further comprising:

setting up a reference data file comprising angle and distance data relating to a plurality of samples of the user's signature inputted during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

35. (Previously presented) The method of claim 34, further comprising:

comparing the angle and distance data extracted from the user's signature inputted during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria.

36. (Previously presented) The method of claim 35, further comprising:

providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison, thereby providing verification of the user's signature.

37. (Previously presented) The method of claim 34, further comprising:

training to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

38. (Currently amended) A computer-readable storage medium having computer-readable instructions stored thereon for authenticating a user's signature, the computer-readable instructions comprising instructions for:

extracting angle and distance data relating to different parts of a user's signature inputted to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and the total time to produce the signature to 1; and

extracting angle and distance data relating to different parts of the normalized signature trace.

39. (Previously presented) The computer-readable medium of claim 38, further comprising instructions for:

setting up a reference data file comprising angle and distance data extracted from a plurality of samples of the user's signature inputted using a manual input device during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

40. (Previously presented) The computer-readable medium of claim 39, further comprising instructions for:

comparing the angle and distance data extracted from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria.

41. (Previously presented) The computer-readable medium of claim 40, further comprising instructions for:

providing an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison, thereby providing verification of the user's signature.

42. (Previously presented) The computer-readable medium of claim 39, further comprising instructions for:

training to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

43. (Currently amended) A system for authenticating a user's signature, the system comprising:

an input apparatus, wherein the input apparatus is configured to provide an output indicative of the location of the input apparatus with respect to time when the input apparatus is manipulated;

a computing apparatus, wherein the computing apparatus is configured to:

extract angle and distance data relating to different parts of a user's signature outputted by the input apparatus to obtain a signature trace;

normalize the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and the total time to produce the signature to 1; and

extract angle and distance data relating to different parts of the normalized signature trace.

44. (Previously presented) The system of claim 43, further comprising:

a reference data file comprising angle and distance data relating to a plurality of samples of the user's signature inputted using a manual input device during a registration phase, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples.

45. (Previously presented) The system of claim 44, further comprising:

a comparator apparatus configured to compare the angle and distance data extracted from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria.

46. (Previously presented) The system of claim 45, further comprising:

an output apparatus configured to provide an output indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison, thereby providing verification of the user's signature.

47. (Previously presented) The system of claim 44, further comprising:

a trainer configured to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

48. (Currently amended) A method of verifying a user's signature, comprising:

comparing angle and distance data from an input signature during an authentication phase to reference angle and distance data, according to defined verification criteria, wherein the angle and distance data comprises extracted angle and distance data relating to different parts of a normalized signature trace, wherein an arc length and total time of the signature trace is normalized to 1 to generate a plurality of temporally equidistant points on the signature trace, and wherein the reference angle and distance data is obtained from a reference data file comprising angle and distance data relating to a plurality of samples of the user's signature, wherein the plurality of samples of the user's signature are normalized based upon a time to obtain a plurality of normalized samples; and

providing an output indicative of an appropriate match between the inputted angle and distance data and the reference angle and distance in dependence on the result of the comparison, thereby providing verification of the user's signature.

49. (Previously presented) The method of claim 48, wherein extracting angle and distance data extracts data relating to different features of the user's signature selected according to the fitness of such features to discriminate the user's signature for the purposes of verification and determined by a fitness function relating the relative fitness of the features to their form and number.

50. (Previously presented) The method of claim 49, wherein the fitness function is optimised by an optimisation algorithm, such as a genetic algorithm.

51. (Previously presented) The method of claim 48, further comprising:

training to refine the verification criteria by which a match is to be judged on the basis of angle and distance data relating to a plurality of samples of the user's signature during the registration phase and generated false samples.

52. (Previously presented) The method of claim 48, further comprising verifying an input of a required password, as determined by reference password, by the user using a keyboard input device.

53. (Previously presented) The method of claim 52, further comprising verifying the input of the password by the user with a required timing, as determined by a reference timing, using the keyboard input device.

54. (Previously presented) The method of claim 53, wherein verifying the input further comprises:

verifying a plurality of hold times for which relevant keys of the keyboard input device are depressed during input of the password; and

verifying a plurality of latency times between the release of one key and the depression of the following key during use of the keyboard input device to enter the password.

55. (Currently amended) A method of verifying a signature, comprising:

receiving, from a manual input device, the signature;

extracting angle and distance data relating to different parts of the signature to obtain a signature trace;

normalizing the signature trace to generate a plurality of temporally equidistant points on the signature trace by normalizing the signature trace to an arc length of ~~the signature trace to~~ 1 and the total time to produce the signature to 1;

extracting angle and distance data relating to different parts of the normalized signature trace;

setting up a reference data file comprising angle and distance data extracted from a plurality of samples of the user's signature inputted into the system by the user during a registration phase;

comparing the angle and distance data extracted from the user's signature inputted into the system during an authentication phase to reference angle and distance data held in the reference data file, according to defined verification criteria; and

providing an output to the user indicative of an appropriate match between the inputted signature to be authenticated and the reference data in dependence on the result of the comparison.